11 mai 2021 | Centre national pour la cybersécurité NCSC

Rapport semestriel 2020/2 (juillet à décembre)

Sécurité de l'information

Situation en Suisse et sur le plan international

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Centre national pour la cybersécurité NCSC

1 Aperçu / sommaire

2 Éditorial

La Suisse a mal à son système de santé

Par Kim Rochat, Co-fondateur de Medidee Services, en charge de l'unité Digital Health

Kim Rochat, Co-fondateur de Medidee Services, en charge de l'unité Digital Health

Le domaine de la santé évolue rapidement grâce à la mise en œuvre de technologies de pointe. La digitalisation des applications, des services, le traitement de plus en plus pointu des données, le recours à l'informatique mobile, à l'intelligence artificielle et à une interconnexion croissante des systèmes permettent des évolutions notables en matière de capacité de soins, de personnalisation de la médecine et ceci au bénéfice de la population. Le domaine de la santé est de plus en plus connecté, c'est une nécessité, une évolution inéluctable et une formidable opportunité.

Ce domaine est doublement stratégique pour notre pays. D'une part, la capacité hospitalière est une ressource critique qui nécessite une disponibilité permanente pour répondre aux besoins de la population en matière de santé. La pandémie a rappelé l'importance de nos capacités en la matière. Dans le même temps, le domaine de la santé est un secteur clé pour notre économie. La Suisse est dotée depuis longtemps de leaders mondiaux dans le domaine pharmaceutique. À ces derniers, s'ajoutent, désormais des acteurs clés du domaine des dispositifs médicaux. L'industrie Medtech, située entre deux Écoles Polytechniques de renommée internationale, bénéficiant d'un maillage fin de hautes écoles spécialisées, d'universités et de centres de formation professionnelle, représente à ce jour près de 60'000 employés, plus de 15 milliards de francs suisses revenus pour 2.3% de notre PIB.

Nombre de fabricants de la Medtech sont par ailleurs des contributeurs clés pour la cybersécurité de notre système de santé. Le législateur européen l'a bien compris et à partir du 26 mai de cette année, une nouvelle législation, votée en 2017, va entrer en application, le Règlement Européen sur les dispositifs médicaux 2017/745/EU. Il inclut désormais l'obligation faite aux fabricants d'assurer que leurs dispositifs soient sûrs non seulement vis-à-vis des patients et des utilisateurs (safety) mais aussi en matière de protection des données ou de prévention d'usages malveillants (security).

Bien que la Suisse, avec ses tergiversations sur l'accord-cadre, se soit exclue de la reconnaissance mutuelle (MRA) en matière de dispositifs médicaux avec l'Europe ; elle a malgré tout décidé de rester alignée sur le droit européen au travers de sa nouvelle ordonnance sur les dispositifs médicaux (ODim). Cette ordonnance, qui entrera en vigueur le 26 mai 2021, renvoie directement au droit européen dans son article 6. Il est donc utile de rappeler que les fabricants suisses doivent désormais assurer la cybersécurité des dispositifs qu'ils mettent sur le marché et il serait utile de s'assurer que ces derniers soient en mesure de répondre rapidement à cette nouvelle obligation.

De plus, la Suisse a été plus créative en introduisant dans son article 74 de cette ODim, l'obligation faite aux établissements de santé «de prendre toutes les mesures techniques et organisationnelles nécessaires conformément à l'état de la technique pour protéger les dispositifs pouvant être connectés à un réseau contre les attaques et les accès électroniques». Au-delà du fait que cet article soit une nouvelle confirmation du retard qu'a le législateur sur la technique, il pose une difficulté à nos institutions de santé en n'adressant que partiellement le fond du problème. Bien qu'il soit indiscutable que les établissements de santé doivent impérativement protéger leurs systèmes d'information de manière robuste et efficace, ces institutions sont souvent incapables de se prémunir face aux risques que certains dispositifs médicaux leur font courir. En effet, bon nombre de dispositifs ne sont pas conçus pour assurer un niveau de sécurité approprié ou les institutions de santé n'ont pas les moyens de remplacer les dispositifs obsolètes. Lors d'un projet auquel j'ai participé dans un hôpital régional, plus de 30 systèmes étaient connus pour être technologiquement obsolètes avec parmi ces derniers des respirateurs et des pompes à infusion, faisant courir un risque inacceptable aux patients.

Le domaine de la santé en Suisse, comme en Europe, a un urgent besoin de faire évoluer ses infrastructures. Dans le même temps, les changements réglementaires en cours et l'accélération de la digitalisation des soins offrent une opportunité formidable à notre industrie. Nos voisins français ont bien compris ce challenge. Le 18 février, leur Président a annoncé une nouvelle stratégie pour développer le secteur de la Cybersecurité avec une allocation d'un milliard d'euros dans la filière cyber notamment en créant un Campus Cyber. Dans ce plan, 515 millions d'euros sont alloués aux développements de solutions souveraines et 176 millions d'euros sont alloués aux besoins du secteur public, notamment les hôpitaux et les collectivités.

En Suisse, le plan stratégique SNPC 2.0 est un progrès notable en la matière, il fixe des objectifs pertinents. Nous bénéficions aussi de l'excellent travail de certains acteurs tels que le Centre National pour la Cybersécurité (NCSC) et assistons à des initiatives heureuses comme le campus cyberdéfense (CYD), mais il est nécessaire que notre stratégie numérique soit beaucoup plus ambitieuse et agressive en matière de sécurité et que notre pays se donne des moyens à la hauteur des enjeux. Nos gouvernants doivent assurer un leadership solide tout en incluant de manière plus structurée et systématique les différents acteurs dans la mise en œuvre de ces systèmes d'information en soutenant de manière encore plus active la recherche, l'industrie et les systèmes de santé à converger vers des solutions communes. Comme nous le rappelle régulièrement les hôpitaux qui font face à des attaques au ransomware (la France en a subi plusieurs récemment), des services critiques pour la population peuvent être mis hors service par des bandes criminelles. Ce risque est connu et il est inacceptable que dans une démocratie telle que la nôtre, il puisse se matérialiser.

Faire émerger les prochaines licornes nationales de la cybersécurité, en mettant à profit nos compétences universitaires, nos infrastructures nationales, pour appuyer notre système de santé à se prémunir des risques qui s'accélèrent, tel est le défi qui doit être relevé sans délai par nos politiques, et il faut plus que des petits pas pour l'adresser.

3 Thème prioritaire: la santé numérique

3.1 Introduction

La transformation numérique progresse inexorablement dans le secteur de la santé aussi, avec ses avantages et ses inconvénients. Les chaînes d'approvisionnement mondialisées et la gestion logistique informatisée sont à l'ordre du jour. Les dossiers des patients sont gérés sous forme numérique, ce qui permet non seulement d'économiser de l'espace de stockage et de sauvegarder les données à un faible coût, mais aussi de transmettre commodément l'anamnèse des patients aux médecins traitants. Or comme dans d'autres domaines, la numérisation croissante étend la surface d'attaque potentielle.

3.2 Données des patients

Les données personnelles sur la santé constituent selon la loi sur la protection des données des «données sensibles» et doivent dès lors être soigneusement protégées contre tout accès non autorisé. Elles sont uniques et en cas d'utilisation abusive, on ne peut pas les remplacer comme un mot de passe. Il faut encore dûment protéger les données sur la santé du risque de destruction, sachant qu'il n'est plus possible de reconstituer les résultats d'anciens examens. La transformation numérique réduit toutefois un tel risque. Les données doivent par ailleurs être protégées contre toute modification non autorisée. L'administration de sang du mauvais groupe peut être fatale à un patient. Des informations erronées sur les intolérances aux médicaments ou les allergies auront des conséquences désastreuses. Seuls les ayants droit autorisés doivent pouvoir accéder à de telles données, et il faut limiter autant que possible le cercle des personnes habilitées à les modifier.

3.3 Dispositifs médicaux numériques

Les dispositifs médicaux sont devenus entre-temps de véritables petits ou grands ordinateurs en réseau. La radiologie numérique gagne du terrain, et les résultats des examens qui n'aboutissent pas directement au réseau d'un cabinet ou d'un hôpital sont stockés dans le cloud. Or expérience à l'appui, les résultats des examens effectués à l'aide de méthodes d'imagerie comme le scanner CT ou la radiographie sont régulièrement archivés – avec les données correspondantes des patients – sur des serveurs cloud mal sécurisés ou des supports de données accessibles depuis Internet[1]. Ce n'est pas tout: plus un appareil d'analyse est grand et compliqué, plus il est susceptible de comporter une interface permettant à son fabricant d'en surveiller le fonctionnement et d'en assurer la maintenance à distance, en cas de besoin.

Le secteur de la santé doit encore apprendre à gérer les risques inhérents à sa mise en réseau systématique avec accès à distance aux données numériques, et établir la culture correspondante. En Allemagne, l'Office fédéral de la sécurité des technologies de l'information (BSI) a signalé, dans le rapport final[2] du projet «ManiMed» (*Manipulation von Medizinprodukten*), que

---

1 Voir ci-après chap. 4.6.3 et rapport semestriel MELANI 2019/2, chap. 4.5.1.

2 ManiMed Abschlussbericht (bsi.bund.de)

tous les produits examinés comportaient des vulnérabilités. Dans presque tous les cas, c'est la sécurité informatique qui était en jeu et pas directement celle des patients.

3.4 Traces des données de dispositifs médicaux

Outre les appareils, les dispositifs médicaux incluent une grande quantité d'ustensiles médico-techniques[3], dont toutes sortes de consommables destinés aux examens et opérations. Divers produits jetables à usage invasif font ainsi l'objet d'un suivi, dans une optique d'assurance-qualité. Tous les cas d'utilisation de produits coûteux et ne se conservant pas indéfiniment sont par ailleurs consignés, car les stocks sont limités et de nouvelles commandes doivent pouvoir être passées à court terme. Les implants médicaux tels que les prothèses de la hanche ou du genou figurent dans le registre suisse des implants (SIRIS)[4]. Cette approche sert aussi à l'assurance-qualité. Le registre doit permettre d'évaluer la qualité à long terme des implants ou celle des traitements. Il remplit encore la fonction de système d'alerte précoce, en cas de défaillance d'un produit ou d'un processus.

La traçabilité des produits utilisés pour les examens et les traitements est un précieux gage de sécurité pour la santé des patients. Il convient par ailleurs de veiller à la confidentialité et à l'intégrité des données enregistrées et à ce titre, les accès ainsi que la manière dont les données sont traitées doivent être retraçables.

3.5 Cybermenaces

Les hôpitaux et autres prestataires du secteur de la santé sont soumis aux mêmes cybermenaces que toute entreprise reliée à Internet et travaillant avec des ordinateurs. Il convient par conséquent de protéger autant que possible, dans le secteur de la santé, les accès aux données et systèmes par une authentification à plusieurs facteurs, afin de prévenir les infections par des maliciels ou du moins de les détecter aussitôt et d'y remédier. Une mesure de protection essentielle consiste en outre à sensibiliser le personnel aux règles de sécurité à observer lors de l'utilisation de ressources informatiques et à le mettre en garde contre les cybermenaces telles que l'ingénierie sociale.

Les menaces ont beau être similaires sinon identiques dans la plupart des secteurs, les attaques fructueuses menées dans le secteur de la santé ont des conséquences bien particulières. Les pertes de données affectent en général des données personnelles non modifiables et sensibles, tandis qu'une panne informatique ou la simple inaccessibilité temporaire des données mettent en péril la santé voire la vie des individus.

3.6 Exemple: chantage reposant sur les données de patients

Depuis quelques années, les rançongiciels (*ransomware*) représentent un modèle d'affaires très prisé des escrocs, qui s'en servent également contre les hôpitaux. Les pirates s'emparent d'un maximum de données avant le cryptage, afin d'avoir un moyen de chantage supplémentaire. Des maîtres chanteurs ont ainsi vainement tenté d'extorquer de l'argent à une clinique

---

3 Ordonnance sur les dispositifs médicaux (ODim, RS 812.213), art. 1.

4 Willkommen beim Schweizer Implantat-Register SIRIS - SIRIS IMPLANT (siris-implant.ch)

de psychothérapie finlandaise, en menaçant de publier les données de ses patients et le contenu des entretiens thérapeutiques. Par la suite, les criminels ont tenté d'opérer ce chantage directement auprès des patients concernés.[5]

3.7 En période de pandémie

Pendant une pandémie[6], les cas de maladie sont susceptibles d'augmenter très vite et d'engorger le système sanitaire. Si de surcroît des cyberincidents perturbent le bon fonctionnement des acteurs du secteur de la santé, des conséquences fatales sont à craindre. L'incident survenu à la clinique universitaire de Düsseldorf, victime d'un rançongiciel en septembre 2020, a fait le tour du monde[7].

En été 2020 déjà, le groupe Hirslanden avait été victime d'un rançongiciel. Des sauvegardes ont toutefois permis de restaurer les données cryptées et à aucun moment, les soins n'ont été menacés[8]. Deux autres hôpitaux helvétiques ont repéré à temps la présence du logiciel «Emotet»[9] et neutralisé l'infection.

Le personnel du secteur de la santé, fortement sollicité pendant une pandémie, est bien souvent au bord de l'épuisement. Il risque d'autant plus de se faire piéger par les méthodes d'ingénierie sociale qu'il est déjà sous pression à cause de circonstances extérieures. De telles cyberattaques jouent notamment sur le sentiment d'urgence des victimes, qu'elles renforcent astucieusement. Le risque dans la précipitation de cliquer sur un lien malveillant figurant dans un courriel ou d'ouvrir une annexe infectée augmente. Il convient donc non seulement de mettre en place des mesures techniques, mais de sensibiliser l'ensemble du personnel aux risques inhérents à l'ingénierie sociale. Il faut en particulier établir des processus administratifs qui permettent de détecter les tentatives de fraude et les autres attaques d'ingénierie sociale.

Recommandation / Conclusion:

Il ne suffit pas de concevoir, au fil de la transformation numérique, de nouvelles solutions d'assistance technique répondant aux meilleures normes de sécurité. Il faut encore apprendre aux utilisateurs à s'en servir de manière correcte et sûre. Les outils numériques sont devenus indispensables dans le secteur de la santé comme dans la vie de tous les jours, et ils vont encore gagner du terrain.

---

5 Vastaamo fires CEO for hiding another data breach in March 2019 (foreigner.fi); Cyber-Erpresser in Finnland: Willkommen in der Dystopie (sueddeutsche.de)

6 Voir aussi le thème prioritaire traité au chap. 3 du rapport semestriel MELANI 2020/1.

7 Uniklinik Düsseldorf: Ransomware "DoppelPaymer" soll hinter dem Angriff stecken (heise.de)

8 Hirslanden von Cyberangriff getroffen: Bedrohung bleibt hoch (nzz.ch)

9 Voir chap. 4.3.2.

4 Situation

4.1 Aperçu des annonces faites au NCSC

Au deuxième semestre 2020, le guichet unique du NCSC a enregistré au total 5542 annonces émanant de particuliers ou d'entreprises[10].

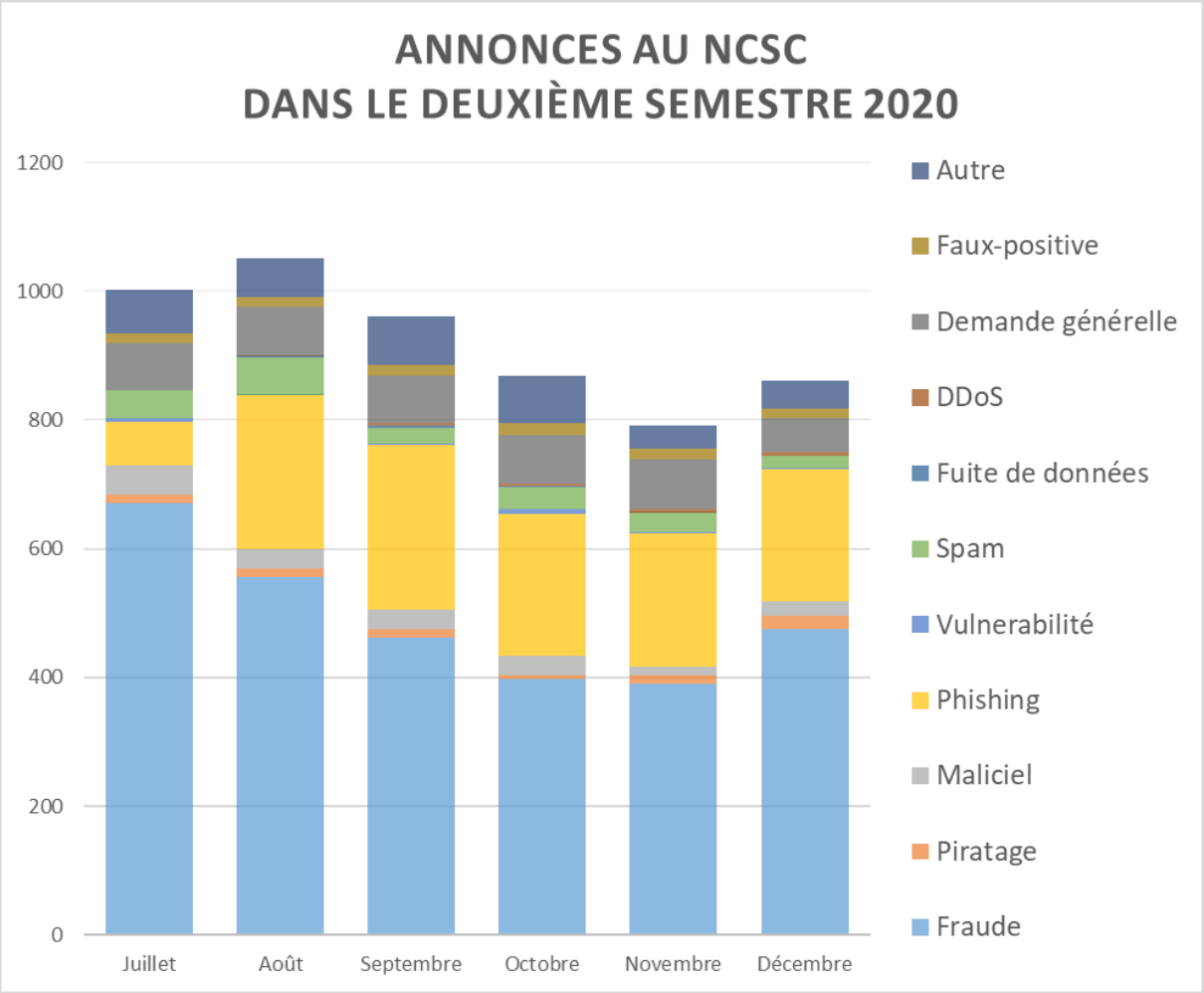


Fig. 1: Signalements effectués au NCSC au deuxième semestre 2020.

Les fraudes représentent toujours la majeure partie des incidents, avec 2917 signalements. La fraude sur Internet a notamment revêtu les formes suivantes:

Fraude au paiement anticipé:

Il s'agit toujours de la variante la plus répandue: 1120 cas de fraude au paiement anticipé ont été signalés au NCSC[11]. Or de tels courriels ont beau être envoyés à grande échelle, leurs chances de succès sont minimes. Dans un seul des cas signalés, le destinataire s'est laissé piéger et a subi un dommage financier.

[10] Les statistiques sont publiées sur notre site: Chiffres actuels (ncsc.admin.ch).

[11] Voir les informations de notre site concernant la fraude au paiement anticipé (ncsc.admin.ch)

Fake-Sextortion:

Des courriels de *fake sextortion*[12] ont été signalés à 353 reprises. Ils prétendent que des photos ou des vidéos montreraient leur destinataire surfant sur des sites pornographiques. Toutes sortes de méthodes visent à convaincre la victime de la véracité de tels propos. Dans une variante, les maîtres chanteurs se servent de l'adresse de leurs victimes, afin qu'elles s'imaginent qu'ils ont pris le contrôle de leur compte de messagerie., alors qu'ils se sont contentés de falsifier l'expéditeur. Dans une autre variante, un mot de passe du destinataire est mentionné comme moyen de preuve. De tels mots de passe proviennent toutefois de fuites d'informations anciennes[13].

Piège d'abonnement:

210 annonces reçues font état de prétendues frais à régler. Il s'agit en général de courriels signalant l'arrivée d'un paquet. Le NCSC a reçu quelque 180 signalements de messages censés émaner de l'Administration fédérale des douanes (AFD) et réclamant d'ordinaire des droits de douane de 75 francs. Le destinataire est prié d'acheter une carte à prépaiement «paysafecard» et d'indiquer son numéro par courriel. De nombreux courriels de la même veine sont envoyés au nom d'entreprises de livraison comme la Poste, DHL ou DPD et invitent à s'acquitter d'une taxe modique par carte de crédit afin de recevoir un paquet[14].

Fraude aux petites annonces, fake support, arnaque au président:

Outre 145 cas d'arnaque aux petites annonces[15] et 130 cas de fake support[16], 111 cas d'arnaque au président[17] ont été recensés. Dans de tels cas, les agresseurs se procurent dans différentes sources en libre accès les informations utiles sur une entreprise ou association, puis cherchent à amener leur correspondant, en falsifiant l'adresse de l'expéditeur, à leur faire un paiement prétendument urgent.

4.2 Nouveau formulaire d'annonce

Le nouveau formulaire d'annonce du NCSC est en ligne depuis le 21 décembre 2020. Il suffit de répondre à quatre questions au maximum pour obtenir une première évaluation automatisée renfermant des informations utiles. Cette assistance technique permet de faire rapidement et commodément une annonce, et aussi de classifier les incidents. Chacun peut encore s'il le désire fournir d'autres indications qui permettront au NCSC de soutenir encore mieux l'auteur de l'annonce, le cas échéant. Les annonces transmises par la population aident le NCSC à repérer rapidement les tendances, à adopter des mesures appropriées à temps ainsi qu'à dresser un tableau complet de la situation au niveau cyber.

---

12 Informations publiées sur notre site à propos de la menace de Fake Sextortion (ncsc.admin.ch)

13 Voir Have I Been Pwned: Check if your email has been compromised in a data breach (havibeenpwned.com)

14 Voir chap. 4.8.2.

15 Informations publiées sur notre site à propos de la fraude aux petites annonces (ncsc.admin.ch)

16 Informations publiées sur notre site à propos du Fake Support (ncsc.admin.ch)

17 Informations publiées sur notre site à propos de l'arnaque au président (ncsc.admin.ch)

4.3 Maliciels

4.3.1 Rançongiciels

Les chevaux de Troie verrouillant les données (rançongiciels) sont ceux qui occasionnent le plus grave préjudice. Au deuxième semestre 2020, le NCSC a reçu 34 annonces provenant de divers secteurs économiques. Près de 80 % des incidents signalés concernaient de petites et moyennes entreprises (PME).

De précédents rapports semestriels ont régulièrement parlé des rançongiciels, qui chiffrent et rendent inutilisables les données de leurs victimes qui sont ensuite priées de verser une rançon aux escrocs pour pouvoir les récupérer . Comme il existe bien souvent des copies de sauvegarde des données et les victimes refusent de payer, les criminels ont mis au point une tactique à double détente. Avant de procéder au chiffrement, ils dérobent les données de la victime. Si leur chantage n'a pas l'effet voulu, ils menacent de publier les données volées ou de les vendre sur le marché clandestin.

Les incidents dus aux rançongiciels peuvent gravement perturber les processus d'exploitation d'une entreprise. La menace risque de devenir existentielle, au cas où la copie de sauvegarde aurait été cryptée au passage. Les pannes de système et donc l'indisponibilité de l'information coûtent très cher, tout comme la gestion des incidents. Dans de telles circonstances, les victimes n'ont pas toutes la même stratégie de communication à l'égard de leurs clients ou partenaires. La palette va du mutisme complet à une publication transparente des faits survenus.

Recommandations:

Les rançongiciels peuvent causer des dommages considérables, en particulier si les copies de sauvegarde (*backups*) sont affectées. En pareil cas, il convient de garder son calme et d'agir de façon réfléchie. Il est important, dans le cadre de la gestion des incidents, d'identifier le canal d'infection et de prévenir toute réinfection. Réinstallez les systèmes concernés et récupérez les données à partir des copies de sauvegarde existantes.

Si votre entreprise ne possède pas les connaissances nécessaires, adressez-vous à une société spécialisée.

Autres informations publiées sur le site du NCSC: Rançongiciels (ncsc.admin.ch).

Incidents survenus en Suisse et au niveau international

En Suisse, les principales entreprises ayant rendu public un incident de rançongiciel au deuxième semestre 2020 sont le géant horloger Swatch Group[18], le constructeur d'hélicoptères Kopter[19], l'entreprise électrique Huber + Suhner[20] et le groupe médical Hirslanden[21].

[18] Swiss watchmaker Swatch shuts down IT systems to stop cyberattack (bleepingcomputer.com)
[19] Ransomware hits helicopter maker Kopter (zdnet.com)
[20] Huber + Suhner von Cyberattacke lahmgelegt (inside-it.ch)
[21] Hirslanden von Cyberangriff getroffen: Bedrohung bleibt hoch (nzz.ch)

Au niveau international, le prestataire de services informatiques Sopra Steria[22] a subi lors d'une panne des dommages qui pourraient grimper à 50 millions d'euros. Un autre cas révélateur s'est produit en Allemagne, dans le secteur de la santé: les données de la clinique universitaire de Düsseldorf[23] ont été chiffrées. La lettre de rançon des maîtres chanteurs est toutefois allée à l'université, qui était en réalité la cible des cybercriminels. Des instituts de formation ont également été touchés à plusieurs reprises aux États-Unis. Les propriétaires du rançongiciel ont dérobé au passage des données confidentielles d'élèves et menacé de les publier si les institutions ne versaient pas la rançon demandée[24].

Nouvelle escalade dans la tactique de chantage par rançongiciel

Pour faire pression sur leurs victimes, certains opérateurs de rançongiciels téléphonent désormais aux entreprises piratées. Ils les menacent par exemple de signaler aux médias la faille de sécurité découverte dans leurs systèmes, ou de publier des documents sensibles sur des sites de divulgation de données (*dedicated leak site, DLS*).

Les exploitants de rançongiciels améliorent leur résilience

De nombreux exploitants de rançongiciels emploient déjà la tactique à double détente du chiffrement et du vol des données. Ils veillent à mettre leurs sites de divulgation de données à l'abri d'un retrait du réseau (*take down*) ordonné par les autorités de poursuite pénale. Leurs infrastructures sont ainsi hébergées dans des pays dont les autorités de poursuite pénale sont peu coopératives. En outre, les données dérobées font souvent l'objet de répliques sur plusieurs serveurs. Une intervention contre un seul serveur ne suffit donc pas à retirer les données du réseau.

Le groupe «Egregor» marche sur les traces de «Maze»

Ce groupe semble être actif depuis septembre 2020. Il s'est attaqué le mois suivant à quelques cibles essentiellement américaines, dont le libraire «Barnes & Noble»[25] et les développeurs de jeux vidéo Ubisoft et Crytek[26]. Puis les attaques se sont multipliées, perturbant par exemple l'exploitation du métro de Vancouver[27]. «Egregor» semble vouloir combler le vide laissé par l'arrêt manifeste, en octobre 2020, des activités du gang «Maze». «Egregor» n'a apparemment pas fait de victimes en Suisse l'année dernière.

Un gang pirate un compte Facebook pour publier ses menaces de chantage

Le producteur italien de spiritueux Campari a été victime d'un rançongiciel. Les agresseurs ont publié sur son compte Facebook, après l'avoir piraté, des menaces de divulgation de données au cas où la rançon ne serait pas versée. La publicité Facebook était désormais intitulée «Faille de sécurité dans le réseau du Groupe Campari», et le gang Ragnar-Locker y signalait que d'autres informations confidentielles seraient publiées.

---

22 Cyber-Attacke kostet Sopra Steria bis zu 50 Millionen Euro (inside-it.ch)

23 Uniklinik Düsseldorf: Ransomware "DoppelPaymer" soll hinter dem Angriff stecken (heise.de)

24 K12 education giant paid the ransom to the Ryuk gang (securityaffairs.co)

25 Cyber-Attack on Major US Bookseller (infosecurity-magazine.com)

26 Ubisoft, Crytek data posted on ransomware gang's site (zdnet.com)

27 Vancouver Metro Disrupted by Egregor Ransomware (threatpost.com)

Cette nouvelle tactique, consistant à publier sur Facebook les attaques commises, illustre le développement continuel des méthodes de chantage auquel se livrent les opérateurs de rançongiciels[28].

4.3.2 «Emotet»

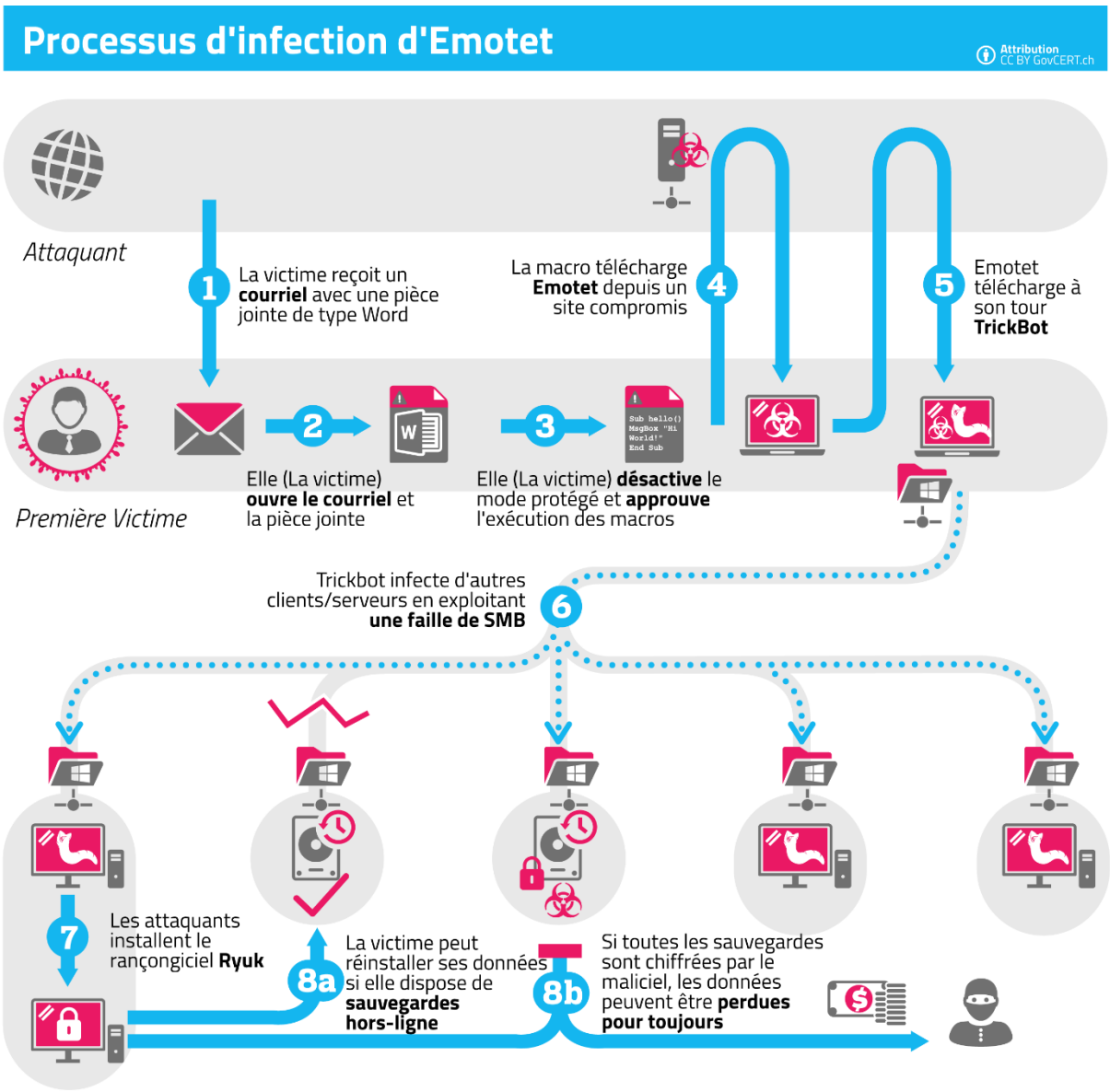


Fig. 2: Processus d'infection d'Emotet

Le NCSC a constaté qu'après s'être fait discret pendant plusieurs mois, le maliciel «Emotet» a déferlé à nouveau depuis juillet 2020, par vagues. En dépit d'une activité moindre qu'au premier semestre, il comptait à nouveau parmi les maliciels les plus répandus, en Suisse et au niveau international[29]. Connu à l'origine comme cheval de Troie bancaire, «Emotet» sert entre-temps aussi à l'envoi de pourriels et au téléchargement de maliciels supplémentaires.

---

28 Ransomware Group Turns to Facebook Ads (krebsonsecurity.com)

29 Voir URLhaus Statistics (abuse.ch)

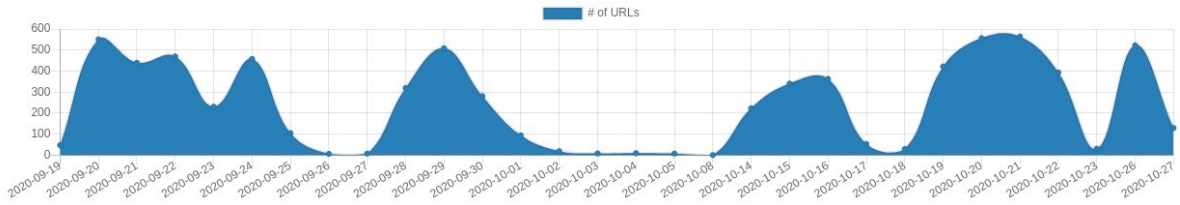


Fig. 3: Nombre d'URL observées servant à télécharger Emotet; vagues d'activité du maliciel

Le NCSC a mis en garde[30] en novembre 2020 contre l'activité d'«Emotet», activement utilisé pour infecter les postes de travail et les serveurs des réseaux avec un rançongiciel comme «Ryuk». Seuls les ordinateurs ou serveurs utilisant le système d'exploitation Windows sont touchés.

Les autorités de huit pays (Pays-Bas, Allemagne, France, Lituanie, Canada, États-Unis, Grande-Bretagne et Ukraine) ont neutralisé ensemble l'infrastructure d'Emotet, selon un communiqué publié le 27 janvier 2021[31]. L'opération «LADYBIRD» semble porter ses fruits, puisqu'elle a durablement mis hors d'état de nuire le réseau de zombies. «Emotet» est toutefois connu pour alterner des phases dynamiques et de longues pauses. Il se pourrait donc que ses créateurs parviennent à mettre en place de nouvelles infrastructures et à reprendre leurs activités criminelles.

Recommandations:

- Empêcher par des moyens techniques l'exécution des macros Office non signées. Il s'agit de repérer au stade de la passerelle de messagerie, à l'aide d'un filtre antipourriel, les documents Office contenant des macros et de ne pas les transmettre aux destinataires. Les fichiers ZIP protégés par mot de passe seront également interceptés et vérifiés avant d'être acheminés à bon port.
- Bloquer les pages Internet utilisées pour propager «Emotet» au niveau du périmètre réseau. Une liste des sites utilisés est fournie gratuitement par URLhaus (abuse.ch).
- Bloquer les serveurs utilisés pour administrer les machines infectées par Emotet. Une liste d'adresses IP liées à «Emotet» est notamment publiée dans le cadre du projet Feodo Tracker (abuse.ch).

Vous trouverez sur notre site des mesures complémentaires et des informations détaillées:

Sécurité de l'information: aide-mémoire pour PME (ncsc.admin.ch)

Mise à jour rançongiciels: nouvelle façon de procéder (ncsc.admin.ch)

30 Trojaner Emotet wieder aktiv (ncsc.admin.ch)

31 World's most dangerous malware EMOTET disrupted through global action (europol.europa.eu)

4.3.3 «Trickbot»

«Trickbot» est demeuré au deuxième semestre 2020 une menace sérieuse pour les entreprises et les organisations. Depuis son apparition en 2016, ce maliciel s'est spécialisé dans la fourniture de logiciels malveillants, servant principalement à rançonner ses victimes[32]. Plusieurs acteurs de la cybersécurité ont tenté à la mi-octobre de démanteler le réseau de contrôle de «Trickbot»[33]. Ces opérations n'ont toutefois eu qu'un effet limité et n'ont pas empêché «Trickbot» de sévir à nouveau.

4.4 Attaques contre des sites ou services Web

4.4.1 Attaques DDoS

Les criminels commencent souvent par lancer une attaque DDoS de démonstration assez brève contre une cible, afin d'apporter la preuve de leur savoir-faire. Ils envoient ensuite un courriel de chantage renfermant une demande de paiement en cryptomonnaie (par ex. bitcoin). Les maîtres chanteurs affirment disposer d'une capacité d'attaque bien supérieure à celle déployée dans leur démonstration de force, et menacent de passer à l'acte. Or dans la plupart des cas, rien ne se passe. D'autres cyberattaques suivent à titre exceptionnel – notamment dans les cas où les premières attaques ont causé d'importantes nuisances. Elles n'ont toutefois jamais l'ampleur annoncée. Comme au premier semestre 2020[34], de telles attaques ont à nouveau augmenté au deuxième semestre sur le plan international. Les analystes de Nexusguard[35] ont fait état d'une croissance des attaques DDoS de 287 % au troisième trimestre, par rapport à la même période de l'année précédente.

Depuis août, une campagne mondiale d'attaques DDoS lancées à des fins de chantage a été constatée dans divers secteurs économiques. Le FBI a même averti les entreprises américaines qu'en l'espace de six jours, des milliers d'organisations du monde entier actives dans toutes sortes de branches avaient reçu des menaces d'attaques DDoS.

Le NCSC n'avait pas constaté de hausse significative des attaques au premier semestre 2020. Les choses ont bien changé au deuxième semestre, où la vague mondiale d'attaques DDoS n'a pas épargné la Suisse. C'est ainsi qu'en août divers secteurs économiques, à commencer par le secteur financier et celui de l'énergie, ont subi des attaques DDoS associées à des demandes de rançons. Durant la période sous revue, 19 attaques DDoS ont été signalées, pour un volume maximum de trafic oscillant entre 150Gbit/s et 200Gbit/s. Les agresseurs se sont souvent parés, dans leurs courriels de chantage, du nom de groupes étatiques célèbres comme «Lazarus» ou «FancyBear» pour intimider leurs victimes et leur faire délier les cordons de leur bourse. En novembre, les escrocs sont revenus à la charge et ont parfois tenté de racketter (à nouveau en vain) les mêmes entreprises.

---

32 Voir rapports semestriels MELANI 2018/2, chap. 4.5.4; 2019/1, chap. 3.4.1 et 4.6; 2019/2, chap. 4.6.1, ainsi que Blogpost Trickbot - An analysis of data collected from the botnet (govcert.admin.ch)

33 Attacks Aimed at Disrupting the Trickbot Botnet (krebsonsecurity.com);
Cyber Command, Microsoft take action against Trickbot botnet before Election Day (cyberscoop.com);
Microsoft and others orchestrate takedown of TrickBot botnet (zdnet.com)

34 Voir rapport semestriel MELANI 2020/1, chap. 4.2.2.

35 DDoS Threat Report 2020 Q3 (nexusguard.com)

Conclusion / Recommandations:

Le chantage DDoS représente une activité de masse. Les pirates tentent leur chance auprès d'un maximum d'entreprises choisies un peu au hasard. Si la manœuvre échoue, ils poursuivent leur quête ailleurs. À supposer qu'une attaque DDoS (de démonstration) ait réussi à bloquer les systèmes d'une entreprise, cette dernière est considérée comme victime potentielle et les escrocs redoublent d'efforts, dans l'espoir qu'une rançon leur soit versée. Il est par conséquent conseillé de bien se préparer à d'éventuelles attaques DDoS.

Le NCSC recommande de conclure pour les systèmes critiques un abonnement à un service commercial de protection DDoS (*DDoS Mitigation Service*). Beaucoup de fournisseurs d'accès à Internet proposent une telle prestation, moyennant un forfait.

Notre site indique diverses mesures utiles pour prévenir et repousser les attaques DDoS: Attaque affectant la disponibilité (attaque DDoS) (ncsc.admin.ch)

4.4.2 Sites Internet compromis

Les pirates peuvent accéder à l'administration des sites Internet pour y installer du code malveillant, en se servant de données d'accès dérobées ou en exploitant des failles de sécurité n'ayant pas été corrigées.

Les conséquences sont très diverses pour les sites Web compromis. Il faut garder à l'esprit qu'en cas de compromission, il n'est plus possible de garantir la confidentialité et l'intégrité des données saisies et sauvegardées.

La division du travail pratiquée sur le marché clandestin amène régulièrement divers acteurs à exploiter les mêmes sites compromis. Il est en effet possible de vendre et d'offrir à plusieurs reprises l'accès en mode administrateur au même site Web. Si le vecteur d'attaque est une faille de sécurité, différents acteurs pourront ainsi compromettre le site Web indépendamment les uns des autres. Il est par conséquent très difficile pour les administrateurs de sites Web d'éradiquer tout code malveillant lors de leur nettoyage.

Recommandations:

Si un site Web a été piraté, il faut le nettoyer systématiquement, en localisant tout code malveillant avant de l'éliminer. En outre, il convient de toujours utiliser la version la plus récente du système de gestion de contenu (CMS) et des modules d'extension (*plug-ins*). Tous les ordinateurs ayant servi à la gestion du site doivent être analysés et nettoyés de leurs maliciels, le cas échéant. Enfin, il convient de modifier toutes les données d'accès. Vous trouverez d'autres informations encore sur notre site:

Site web piraté – que faire? (ncsc.admin.ch)

Une fois le site Web nettoyé, il est recommandé d'adopter des mesures supplémentaires pour éviter de subir à l'avenir une nouvelle intrusion de cybercriminels. Vous trouverez sur notre site les principales mesures à prendre:

Mesures de protection pour les systèmes de gestion de contenu (ncsc.admin.ch)

4.4.3 Arnaques aux cryptomonnaies (*crypto-scams*)

Le battage médiatique autour des cryptomonnaies a eu toutes sortes de retombées – parfois frauduleuses. Les arnaques aux cryptomonnaies («*crypto-scams*») recouvrent toutes sortes de phénomènes, à l'instar d'offres d'investissement frauduleuses, de fausses plateformes d'échange (avec l'app correspondante) voire de cryptomonnaies factices. Une escroquerie peut aussi débuter à partir d'un compte compromis dans les réseaux sociaux. C'est ainsi qu'en juillet 2020, une attaque spectaculaire a compromis 130 comptes Twitter de personnalités ou d'entreprises en vue[36]. Les comptes de Barack Obama, Joe Biden, Elon Musk, Mike Bloomberg ou Bill Gates ont ainsi publié des tweets promettant une récompense à quiconque effectuerait un versement à l'adresse bitcoin indiquée:

Fig. 4: Exemple de nouvelle publiée à partir d'un compte piraté

L'attaque n'a duré que quelques minutes, qui ont suffi à collecter 180'000 USD sur les comptes en bitcoin des pirates.

4.5 Systèmes de contrôle industriels (SCI)

La gestion numérique des processus physiques contribue largement au confort matériel des sociétés industrialisées. Il est par conséquent tentant pour les cyberpirates de perturber le bon fonctionnement de tels systèmes. De même, il est toujours plus difficile aux exploitants d'en assurer la protection, à l'ère de l'automatisation et du réseautage.

4.5.1 Diversification des menaces

Il a été question, dans de nombreux rapports semestriels, des risques guettant les systèmes de contrôle industriels. L'état des connaissances a progressé ces derniers mois sur certaines sources de menaces, tandis que de nouveaux périls et de nouveaux agresseurs faisaient leur apparition.

---

[36] 2020 Twitter bitcoin scam (en.wikipedia.org)

En octobre 2020, le Ministère américain de la justice a porté plainte contre six membres d'une unité du service de renseignement militaire russe (GRU)[37]. Baptisée «Sandworm» par des chercheurs en cybersécurité privés, cette unité serait notamment à l'origine des pannes électriques survenues en décembre 2015 et en décembre 2016 en Ukraine, ainsi que du virus destructeur «NotPetya». Quelques jours plus tard, le Ministère américain des finances sanctionnait un institut de recherche russe pour sa participation aux attaques du maliciel Triton/Trisis[38]. Ces attaques cherchaient à désinstaller les systèmes instrumentés de sécurité (*safety instrumented system, SIS*) des procédés industriels, censés garantir qu'aucun être humain ou aucune machine ne subisse de préjudice en cas de panne d'une installation. Dans une mise en garde commune[39], le FBI et l'agence de cybersécurité américaine (CISA) ont fait état d'incidents attribués au groupe «Berserk Bear». Même si les autorités américaines n'ont relevé aucune tentative de sabotage de la part des intrus, leur mode opératoire donne à penser qu'ils préparaient le terrain dans cette optique.

Plusieurs attaques visant les systèmes d'irrigation de l'agriculture israélienne seraient dues à des acteurs iraniens[40].

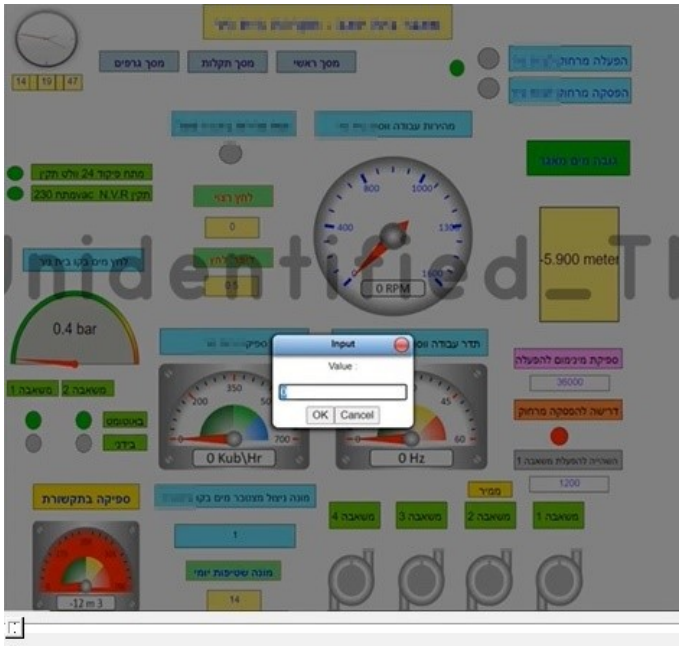


Fig. 5: Séquence de la vidéo de démonstration du système ouvert contrôlant l'approvisionnement en eau.

À l'instar de l'approvisionnement en eau, l'alimentation électrique n'est jamais à l'abri d'un cyberincident. Selon les autorités indiennes, la panne électrique survenue le 13 octobre 2020 à Bombay serait due à une tentative de cybersabotage[41].

---

37 Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace (justice.gov);
US Indicts Sandworm, Russia's Most Destructive Cyberwar Unit (wired.com)

38 US Treasury sanctions Russian research institute behind Triton malware (zdnet.com)

39 Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets (cisa.gov)

40 Two more cyber-attacks hit Israel's water system (zdnet.com);
What We've Learned from the December 1st Attack on an Israeli Water Reservoir (otorio.com)

41 October Mumbai power outage may have been caused by a cyber attack (securityaffairs.co)

Des attaques à mobile politique ou militaire contre les infrastructures critiques continuent d'être observées principalement dans le cadre de conflits qui dégénèrent.

Les rançongiciels s'attaquant aux processus industriels demeurent une menace pour les opérateurs de systèmes de contrôle critiques, comme l'a notamment démontré à plusieurs reprises le maliciel «EKANS»[42].

4.5.2 Défi lié à la protection de la chaîne d'approvisionnement dans la numérisation des processus industriels

Les systèmes de contrôle comprennent différentes composantes issues de fabricants divers ou de projets *open source*. Lorsqu'une défaillance apparaît en amont dans la chaîne d'approvisionnement, les exploitants de systèmes ont souvent du mal à évaluer dans quelle mesure elle affecte leurs commandes, leurs capteurs et leurs actionneurs, et à plus forte raison comment corriger la faille de sécurité dans le système en place.

La question s'est en particulier posée lors de l'identification, dans des projets *open source*, de diverses failles permettant d'utiliser les protocoles réseau de toutes sortes d'appareils. Ces vulnérabilités, baptisées «AMNESIA:33»[43], affectaient une bonne centaine de fabricants de composantes et appareils. Le NCSC a collaboré activement avec les fournisseurs concernés en Suisse, afin que la publication des failles soit dûment coordonnée et que des mises à jour soient disponibles pour tous les produits.

En réponse aux défis complexes auxquels sont confrontés les exploitants d'infrastructures critiques, le NCSC soutient de son expertise l'initiative du canton de Zoug visant à créer un institut national de test pour la cybersécurité (NTC)[44].

4.6 Fuites de données

Le phénomène des fuites de données n'a rien perdu de son actualité et apparaît dans toutes sortes de contextes. Il arrive que les pirates réutilisent eux-mêmes les données dérobées. Or le plus souvent, elles sont vendues sur le marché clandestin ou publiées sur des forums de pirates. De nombreuses fuites de données ne sont découvertes que lorsqu'une telle offre est lancée. Certains acteurs cherchent aussi à mettre leurs victimes sous pression, en les menaçant de publier leurs données. Les opérateurs de rançongiciels ont intégré cette approche dans leur modèle d'affaires, à côté du cryptage des données.

La valeur monétaire élevée de certains types de données, telles les données médicales, les données de clients ou les données d'identification et, dans une moindre mesure, les données bancaires, en fait des cibles convoitées. Les données relatives à la propriété intellectuelle sont également très prisées et donnent lieu à des campagnes avancées d'espionnage.

---

42 This is how EKANS ransomware is targeting industrial control systems (zdnet.com)

43 AMNESIA:33 How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices (forescout.com)

44 Kanton Zug plant nationale Prüfstelle für IT-Hardware (netzwoche.ch); Participation de la Confédération à la création et au fonctionnement de l'institut national de test pour la cybersécurité (parlament.ch)

4.6.1 Vol de données de citoyens suisses en Argentine

À la fin d'août 2020, une attaque de rançongiciel lancée contre les autorités argentines de l'immigration, a abouti au vol des données personnelles de dizaines de milliers de personnes, dont 11'000 ressortissants suisses[45]. Faute du paiement de la rançon demandée, les escrocs ont publié les données dans le Web clandestin. On y trouvait les nom, prénom, date de naissance et numéro de passeport des victimes, avec leur destination, mais sans copie de leur pièce d'identité.

4.6.2 Données d'accès VPN aux mains de pirates

En août 2020, on a découvert que des pirates avaient dérobé les adresses IP, les noms d'utilisateur et les mots de passe de plus de 900 serveurs VPN professionnels utilisant Pulse Secure[46] et les avaient publiés sur un forum de pirates russe. Les données étaient utilisées par des criminels pour lancer des attaques avec un rançongiciel. À la suite de ce vol de données, le NCSC a pris contact avec les entreprises suisses concernées et les a dûment informées de la situation, afin qu'elles puissent modifier les données d'accès divulguées.

4.6.3 Données publiées par mégarde

Loin d'être toujours imputable à une cyberattaque, la divulgation de données sensibles peut aussi bien s'expliquer par une erreur de configuration du propriétaire des données. Selon un rapport de l'entreprise de cybersécurité Risk Based Security, 69 % des fuites de données sont causées par inadvertance par des personnes internes à l'organisation concernée[47]. L'entreprise de sécurité britannique Sophos a ainsi été informée que les données de ses propres clients étaient visibles en ligne[48]. La popularité des plateformes cloud exacerbe encore ce phénomène, car de telles plateformes exigent une configuration irréprochable. Le géant pharmaceutique américain Pfizer a par exemple commis une erreur dans la configuration d'une plateforme Google-Cloud : les données divulguées concernaient des patients ayant notamment subi un traitement anticancéreux[49]. En analysant les ressources d'Internet, la société CybelAngel a découvert au moins 45 millions de photos médicales, avec les données des patients concernés, accessibles à tout un chacun sur plus de 2000 serveurs non protégés[50].

Conclusion / Recommandations:

Une gestion attentive et responsable des données s'avère prioritaire pour les entreprises. En plus d'adopter des mesures de sécurité adéquates, toute entreprise devrait se préparer au scénario d'une fuite de données et élaborer à l'avance un plan de réponse aux incidents (*data breach response plan*), qui lui permette de déployer rapidement une action coordonnée en cas de besoin.

---

45 Argentina hack reveals data on thousands of Swiss travellers (swissinfo.ch)
46 Hacker leaks passwords for 900+ enterprise VPN servers (zdnet.com)
47 2020 Year End Data Breach QuickView Report (riskbasedsecurity.com)
48 Sophos notifies customers of data exposure after database misconfiguration (zdnet.com)
49 Pharma Giant Pfizer Leaks Customer Prescription Info, Call Transcripts (threatpost.com)
50 More Than 45 Million Unprotected Medical Images Accessible Online (cybelangel.com)

Autres informations publiées sur le site du NCSC: fuite de données (ncsc.admin.ch)

4.7 Espionnage

4.7.1 COVID-19 et espionnage

La pandémie de COVID-19 mobilise les chercheurs du monde entier, et une véritable course au vaccin a été engagée. Dès le premier semestre 2020, des mises en garde ont été publiées contre les tentatives d'espionnage[51] et au deuxième semestre, plusieurs cyberattaques ont été publiquement confirmées contre des établissements de recherche et des entreprises pharmaceutiques. Aucune technique ou tactique nouvelle n'a toutefois été observée à ce jour. Les autorités étatiques ont également continué à faire l'objet de campagnes d'espionnage visant, en particulier, leurs procédures d'évaluation des dispositifs médicaux en relation avec le COVID-19.

Le 16 juillet 2020, le Centre britannique de cybersécurité (NCSC-UK) a publié avec le Centre canadien de la sécurité des télécommunications (CSE) et l'Agence américaine de cybersécurité et de sécurité des infrastructures (CISA) un document attribuant les cyberattaques visant la recherche sur le vaccin contre le COVID-19 au groupe «APT29» et incriminant notamment le maliciel «Wellmess»[52]. Le groupe APT29, également connu en tant que «The Dukes» ou «CozyBear», est souvent associé à la Russie[53].

Microsoft a fait état en septembre de campagnes orchestrées contre les institutions de recherche et les entreprises actives dans le développement de vaccins[54] et publié en novembre ses observations sur les cyberattaques menées contre sept entreprises travaillant sur des vaccins[55].

En novembre, l'Agence européenne des médicaments (EMA) a été victime d'une cyberattaque ciblée dont l'origine, l'ampleur et les conséquences restent inconnues, l'enquête n'étant pas terminée[56]. Pfizer et Moderna ont publié des communiqués confirmant que des intrus avaient dérobé dans les systèmes de l'EMA des documents se rapportant au développement de leurs vaccins[57]. Des données pillées à cette occasion sur le vaccin contre le COVID-19 de Pfizer/Biontech ont été publiées sur Internet au début de 2021[58]. L'auteur du piratage n'a pas été identifié à ce jour et l'affaire continue d'être examinée.

---

51 Voir rapport semestriel MELANI 2020/1, chap. 4.6.1.

52 Advisory-APT29-targets-COVID-19-vaccine-development.pdf (ncsc.gov.uk)

53 APT 29 (Threat Actor) (fraunhofer.de)

54 Microsoft report shows increasing sophistication of cyber threats (microsoft.com)

55 Cyberattacks targeting health care must stop (microsoft.com)

56 Cyberattack on the European Medicines Agency (europa.eu)

57 Statement on Cyberattack on the European Medicines Agency (modernatx.com); Statement Regarding Cyber Attack on European Medicines Agency (biontech.de)

58 Hackers leak stolen Pfizer COVID-19 vaccine data online (bleepingcomputer.com)

En décembre, Kaspersky Lab a publié un rapport attribuant au groupe de pirates nord-coréen «Lazarus» des attaques de cyberespionnage lancées en septembre contre un groupe pharmaceutique, ainsi qu'une attaque commise le mois suivant avec différents types de maliciels contre un ministère de la santé[59].

Conclusion:

Quiconque effectue des travaux de recherche sur le COVID-19 doit s'attendre à des attaques d'espionnage d'origines diverses, a fortiori s'il cherche à développer un vaccin. Les données collectées, les résultats des travaux et les secrets commerciaux détenus dans ce secteur intéressent des organisations tant étatiques que privées.

4.7.2 Attaque contre la chaîne d'approvisionnement: SolarWinds Orion IT

Le 13 décembre 2020, plusieurs autorités américaines ont révélé qu'un groupe d'attaquants avait accédé à leur réseau à travers une mise à jour compromise du logiciel Orion IT. La mise à jour officielle du programme avait été modifiée en mars 2020 pour inclure une porte dérobée. Près de 18 000 utilisateurs du logiciel avaient téléchargé la mise à jour frauduleuse. Les agresseurs ont alors recherché des cibles intéressantes pour leurs activités de piratage, refermant la porte dans le cas des victimes collatérales.

Selon des sources américaines, l'opération s'inscrivait dans une vaste campagne d'espionnage prenant pour cibles d'autres entreprises encore, et qui présentait des similitudes avec les pratiques de l'acteur «APT29».

Conclusion / Recommandations:

Les attaquants peuvent se procurer un accès en amont de leur cible, en compromettant un de ses fournisseurs. La stratégie d'attaque de la chaîne d'approvisionnement (*supply chain attack*) gagne du terrain depuis plusieurs années (voir AVAST CC Cleaner, ASUS, Cloudhopper). Elle est d'autant plus intéressante qu'elle livre accès à plusieurs cibles à la fois et permet dans un premier temps de mieux dissimuler l'accès illégitime. Lors de telles campagnes, les agresseurs connaissent d'ordinaire à l'avance leur cible finale, et les fournisseurs ne sont qu'un simple moyen d'arriver à leurs fins. Mais à l'avenir, la méthode d'attaque de la chaîne d'approvisionnement pourrait aussi tenter des agresseurs opportunistes, séduits par l'idée de faire un maximum de victimes.

En plus de se doter d'une base de référence recensant les communications légitimes dans son propre réseau, de façon à pouvoir identifier les anomalies, il est recommandé de dûment définir, lors de la conclusion des contrats de prestations, les informations et alertes à transmettre au cas où un des fournisseurs serait victime d'une cyberattaque.

59 Lazarus covets COVID-19-related intelligence (securelist.com)

4.7.3 Portes dérobées dans des logiciels des impôts chinois

En été 2020, l'entreprise de sécurité Trustwave a découvert deux maliciels du nom de GoldenSpy[60] et GoldenHelper[61] dans un logiciel d'impôt destiné aux entreprises occidentales établies sur sol chinois. Ces programmes permettent d'accéder à distance au système client de la victime. Les clients de Trustwave ainsi piratés comprenaient une entreprise active dans les nouvelles technologies et un grand établissement financier.

Conclusion / Recommandations:

Afin de se protéger des logiciels d'espionnage, les entreprises feraient bien d'installer les logiciels imposés par les autorités sur un ordinateur séparé du reste de leur réseau.

Mesures concrètes à prendre concernant GoldenSpy/GoldenHelper:

- Ajouter à sa propre surveillance des menaces les indicateurs de compromission (*indicators of compromise, IOC*) figurant dans la mise en garde du FBI (et prêter attention aux éventuels nouveaux IOC);
- Entreprises ayant déjà installé ce logiciel: y voir un incident potentiel et se conformer aux instructions de Trustwave.

4.8 Ingénierie sociale et phishing

Les escrocs se livrant au phishing ou à d'autres pratiques d'ingénierie sociale rivalisent d'imagination pour leurs attaques. Ils inventent des histoires plus ou moins originales, avec des événements censés s'être produits dans le cadre familier des victimes.

4.8.1 Aperçu du phishing

Quelque 4'498 sites de phishing signalés sur le portail antiphishing.ch, géré par le NCSC, ont été désactivés au deuxième semestre 2020. Soit une hausse de plus de 30 % par rapport au premier semestre, où 3'029 sites de phishing avaient été annoncés.

Plusieurs campagnes ont imité les messages d'opérateurs de télécommunication: il y était question d'un paiement effectué à double et qui allait être remboursé. D'autres campagnes ont usurpé les logos d'établissements financiers ou d'entreprises de transports publics. Le phishing vise typiquement à subtiliser les données d'ouverture de session d'un portail en ligne, les données de carte de crédit, le numéro de téléphone portable et d'autres informations.

De nombreuses campagnes ont tenté d'intercepter, le cas échéant, le code de sécurité transmis par SMS pour venir à bout de l'authentification à deux facteurs.

60 'GoldenSpy' Malware Hidden In Chinese Tax Software (securityweek.com)

61 Researchers Find More Malware Delivered via Chinese Tax Software (securityweek.com)

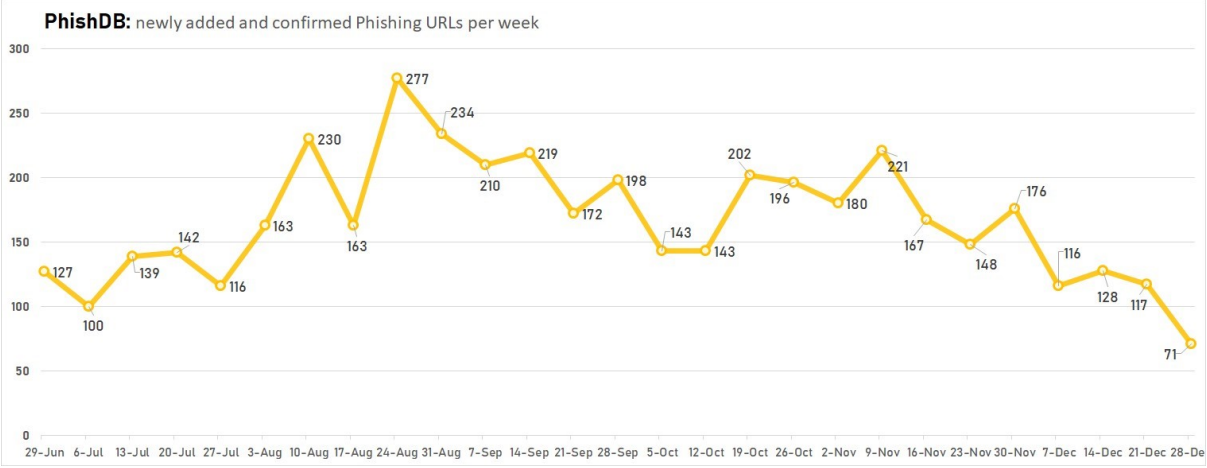


Fig. 6: Nombre d'adresses URL de phishing examinées et confirmées par le NCSC chaque semaine au deuxième semestre 2020. Les données actuelles sont publiées sous: https://www.govcert.admin.ch/statistics/phishing/

Précision:

Informations générales publiées sur notre site: phishing (ncsc.admin.ch)

4.8.2 Phishing reposant sur le scénario de l'envoi d'un colis

Pandémie oblige, les achats en ligne ont augmenté au deuxième semestre 2020. Presque tout le monde était susceptible d'attendre un paquet. Diverses campagnes de phishing par courriel ou SMS ont su tirer parti de cette situation.

Prétendue taxe à régler pour la livraison d'un paquet (par courriel)

Des courriels expédiés au nom d'une célèbre entreprise de livraison signalaient qu'un paquet n'avait pas pu être délivré, en raison d'un problème technique. Il fallait donc régler une taxe pour une nouvelle livraison, afin de recevoir le colis à bref délai (dans les 24 heures). Un lien redirigeait la victime vers un site frauduleux, ressemblant à s'y méprendre à l'original. Il fallait y indiquer, en vue du paiement, son nom et les données de sa carte de crédit. La victime avait l'impression que tout le processus de paiement s'était déroulé correctement. En réalité, les escrocs étaient en mesure d'effectuer des achats à partir de sa carte de crédit, grâce aux données divulguées.

Prétendue taxe à régler à cause d'un paquet bloqué (par SMS)

Dans une autre variante, un SMS censé provenir d'un entreprise de livraison signalait qu'un paquet avait été gardé en dépôt à cause d'un affranchissement insuffisant. Il fallait cliquer sur le lien indiqué pour en confirmer la livraison. Or l'hyperlien du SMS aboutissait à un site Web créé par des cybercriminels, sur lequel la victime était priée d'indiquer ses coordonnées personnelles et les données de sa carte de crédit. Une taxe mensuelle était ensuite débitée de sa carte, et parfois son compte en banque était pillé.

4.8.3 Vol d'identifiants Apple ou installation de logiciels espions

Des SMS dont la teneur était «Vous êtes invité/e à retirer un envoi de LA POSTE» et munis d'un hyperlien conduisaient à des sites Web différents, selon le type de téléphone mobile contacté. Les utilisateurs Apple devaient indiquer leur identifiant Apple sur une page de phishing.

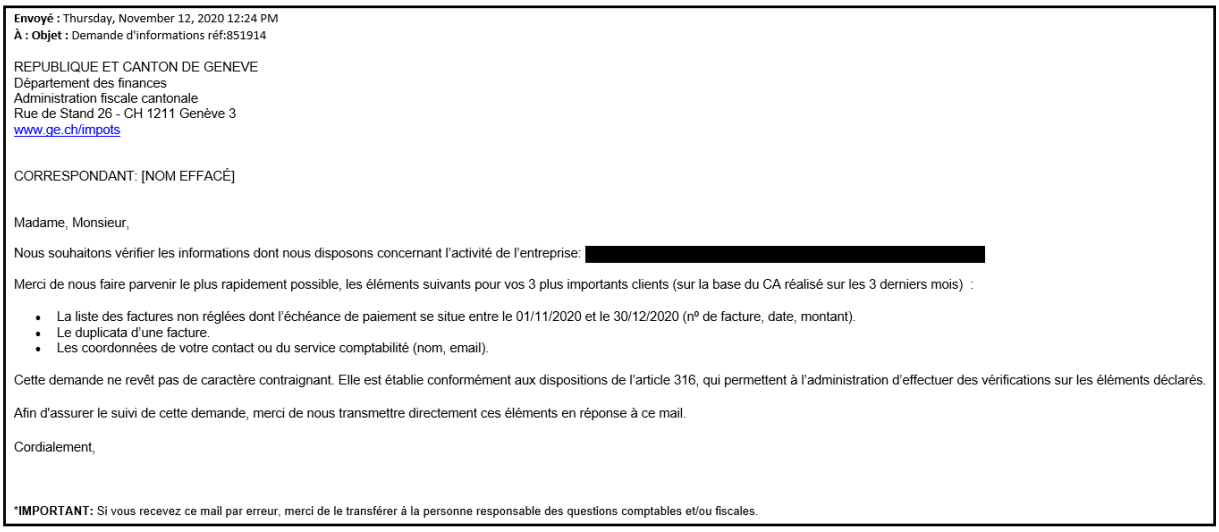
Les utilisateurs d'Android étaient priés d'installer une app. Il s'agissait en réalité d'un logiciel espion, qui dérobait les données et renfermait une porte dérobée (*backdoor*). Les numéros utilisés pour ce genre d'envois provenaient de smartphones infectés, ou alors il s'agissait de numéros falsifiés.

4.8.4 Usage abusif de services Google à des fins de phishing

La société de cybersécurité Armorblox[62] a récemment analysé la manière dont des escrocs piratent divers services Google, lors de leurs campagnes de phishing ou de fraude. La plupart du temps, ces opérations visent à dérober des données sensibles (données d'accès, données bancaires et données personnelles). Comme très peu d'entreprises bloquent les services Google, les agresseurs y ont trouvé une méthode efficace pour contourner les mécanismes de sécurité. Cette tactique est surtout payante en combinaison avec des méthodes avancées d'ingénierie sociale visant par exemple à convaincre les victimes de télécharger un fichier ou de compléter un formulaire.

4.8.5 Usurpation de l'identité d'autorités fiscales

Deux des mécanismes essentiels au succès de l'ingénierie sociale consistent à générer un sentiment de familiarité ainsi qu'à prétexter l'urgence d'agir. À cet effet, les cybercriminels usurpent souvent l'identité de services étatiques, d'autorités fiscales en particulier, pour accéder à des informations sensibles. En novembre 2020, des dizaines d'entreprises ont ainsi reçu des courriels expédiés au nom de collaborateurs de l'administration fiscale du canton de Genève. Il y était question de données de clients et de factures ouvertes. Selon toute probabilité, les escrocs préparaient le terrain à une fraude au virement (*wire fraud*). L'administration fiscale genevoise a mis en garde la population sur son site Internet et dans une lettre d'information.[63] 37 entreprises ont signalé avoir reçu de tels courriels frauduleux.



Envoyé : Thursday, November 12, 2020 12:24 PM
À : Objet : Demande d'informations réf:851914

REPUBLIQUE ET CANTON DE GENEVE
Département des finances
Administration fiscale cantonale
Rue de Stand 26 - CH 1211 Genève 3
www.ge.ch/impots

CORRESPONDANT: [NOM EFFACÉ]

Madame, Monsieur,

Nous souhaitons vérifier les informations dont nous disposons concernant l'activité de l'entreprise: [redacted]

Merci de nous faire parvenir le plus rapidement possible, les éléments suivants pour vos 3 plus importants clients (sur la base du CA réalisé sur les 3 derniers mois) :

- La liste des factures non réglées dont l'échéance de paiement se situe entre le 01/11/2020 et le 30/12/2020 (nº de facture, date, montant).
- Le duplicata d'une facture.
- Les coordonnées de votre contact ou du service comptabilité (nom, email).

Cette demande ne revêt pas de caractère contraignant. Elle est établie conformément aux dispositions de l'article 316, qui permettent à l'administration d'effectuer des vérifications sur les éléments déclarés.

Afin d'assurer le suivi de cette demande, merci de nous transmettre directement ces éléments en réponse à ce mail.

Cordialement,

*IMPORTANT: Si vous recevez ce mail par erreur, merci de le transférer à la personne responsable des questions comptables et/ou fiscales.

Fig. 7: Exemple de courriel d'ingénierie sociale.

62 OK Google, Build Me a Phishing Campaign (armorblox.com)

63 L'AFC met en garde les entreprises contre des tentatives de phishing (ge.ch)

Recommandations:

La prudence s'impose face aux courriels non sollicités. Il convient de vérifier l'expéditeur et la légitimité de l'ordre donné. Faites très attention à la transmission de données sensibles et aux transactions financières. Sensibilisez le personnel de votre service comptable et tous les collaborateurs occupant des positions-clés dans ce contexte. En cas de paiement erroné, adressez-vous immédiatement à votre banque. Le cas échéant, elle aura encore la possibilité de stopper ou d'annuler le paiement.

4.8.6 Harponnage (*spear phishing*)

Le harponnage (*spear phishing*) est une forme d'attaque raffinée, visant à obtenir des informations sensibles de la part de personnes précises. Comme une telle façon d'agir nécessite des ressources considérables et une grande patience, elle émane en général d'acteurs étatiques ou de bandes d'escrocs bien organisées.

Microsoft[64] a par exemple analysé les activités de «Phosphorus». Ce groupe, présenté comme lié au gouvernement iranien, a tenté de soutirer à une centaine d'experts en sécurité les données d'accès de leur compte de messagerie. Concrètement, de fausses plateformes ont été créées pour des conférences internationales sur la sécurité organisées à Munich et en Arabie Saoudite. Après avoir identifié les experts en sécurité qui devaient s'y rendre, les pirates leur ont transmis une fausse invitation. Les destinataires étaient priés d'indiquer des renseignements biographiques, ainsi que leur nom d'utilisateur et leur mot de passe, sur un nom de domaine censé être celui des deux conférences de haut niveau. Ces indications ont permis à Phosphorus d'accéder aux comptes de messagerie de leurs victimes, afin de leur dérober des données.

Dans d'autres attaques de *spear phishing*, les escrocs se sont fait passer pour des recruteurs. Ils contactaient leurs victimes par le réseau professionnel LinkedIn et leur faisaient miroiter un poste intéressant. Divers cybergangs, dont le groupe nord-coréen «Lazarus»[65], ont utilisé cette tactique. Ce dernier groupe étatique a procédé de la manière suivante, au cours de l'opération «Dream Job»:

1. Création d'un faux compte LinkedIn de recruteur d'une grande entreprise connue;
2. Phase exploratoire: collecte d'un maximum d'informations pouvant servir plus tard à piéger la personne prise pour cible;
3. Préparation du «job de rêve»: création d'une fausse offre d'emploi répondant aux aspirations de la victime présumée;
4. Prise de contact avec la victime: le faux recruteur entre en contact avec la personne par l'intermédiaire de son réseau LinkedIn; l'offre d'emploi est évoquée par Whatsapp ou par courriel;
5. Envoi des données détaillées sur l'offre d'emploi dans un fichier Word ou PDF renfermant le maliciel, que la victime pourra télécharger par DropBox ou par OneDrive. Les

64 Cyberattacks target international conference attendees (microsoft.com)

65 Dream-Job-Campaign (clearskysec.com)

pirates choisissent un moment opportun d'un point de vue tactique: la victime doit être au travail quand elle ouvre leur fichier;

6. Phase d'infection: les pirates pénètrent dans le réseau de leur victime;
7. Le faux profil LinkedIn est supprimé et la conversation en reste là.

Une fois dans le réseau d'entreprise, les pirates y déploient des activités d'espionnage ou envoient des courriers frauduleux à partir du compte piraté (*Business-EMail-Compromise, BEC*)[66].

Cette tactique est très raffinée, car elle peut compter sur la discrétion des victimes. Le contexte actuel semble en outre propice, le COVID-19 ayant rehaussé l'attrait des postes sûrs dans les grandes entreprises réputées.

5 Autres thèmes

5.1 Obligation faite aux infrastructures critiques de signaler les cyberattaques

Le Conseil fédéral a pris en décembre 2020 la décision de principe de soumettre les exploitants d'infrastructures de sécurité à une obligation générale de déclarer les cyberattaques dont elles sont victimes ou la détection de failles de sécurité[67].

À ce jour, l'échange d'informations sur les cyberattaques s'effectue sur une base volontaire, par l'intermédiaire du NCSC. Or la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) indique qu'il faut examiner l'introduction d'une obligation de signaler les cyberincidents pour les exploitants d'infrastructures critiques. Le Conseil fédéral a donc chargé le Département fédéral des finances (DFF) de préparer, d'ici à la fin de 2021, un projet qui crée les bases légales nécessaires. Il s'agit de définir, en tenant compte des obligations de déclarer existantes, des critères servant à déterminer qui doit signaler quels incidents, et dans quel délai. Rien ne filtrera sur les auteurs des déclarations qui devront être transmises à une centrale d'enregistrement, selon la volonté du Conseil fédéral.

Les données recueillies dans le cadre des déclarations serviront à diffuser systématiquement des alertes rapides. De tels échanges d'information ont pour but l'identification précoce des méthodes d'attaque ainsi qu'une meilleure évaluation de la menace, et contribueront à renforcer encore la sécurité de la Suisse dans ce domaine.

5.2 Les cantons souhaitent mieux coordonner la lutte contre la cybercriminalité

Les commandants de police des cantons entendent mieux coordonner la lutte contre la cybercriminalité et la pédocriminalité. À cet effet, la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP) a approuvé les termes d'une convention

---

66 Informations publiées sur notre site à propos du piratage d'une messagerie professionnelle (ncsc.admin.ch)

67 Le Conseil fédéral est favorable à ce que les infrastructures critiques soient tenues de signaler les cyberattaques (admin.ch)

conclue avec la Conférence des commandants des polices cantonales de Suisse (CCPCS) en vue de régir l'organisation et le financement d'un réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK). La convention est entrée en vigueur le 1er janvier 2021[68].

La CCPCS a fondé le NEDIK en 2018 déjà. La nouvelle convention administrative régit l'organisation et le financement des prestations fournies dans le cadre du réseau d'enquêtes. Le NEDIK a notamment pour but d'assurer le transfert mutuel de connaissances, d'établir un aperçu national des cas et de permettre la classification des cas à caractère intercantonal. Le NEDIK contribue également à la prévention et collabore avec la Prévention suisse de la criminalité (PSC) et le Centre national pour la cybersécurité (NCSC). Pour lutter efficacement contre la criminalité informatique, le NEDIK utilisera des outils d'analyse spéciaux et gérera une base de données où seront centralisées les connaissances. Au sein du réseau d'enquêtes NEDIK, l'Office fédéral de la police (fedpol) assume enfin un rôle de coordination supracantonale et transnationale, et garantit la coordination des affaires internationales avec les autorités partenaires à l'étranger telles qu'Europol ou Interpol.

5.3 Stratégie de politique extérieure numérique du Conseil fédéral

La transformation numérique offre de nouvelles opportunités à la Suisse et à sa politique extérieure. En effet, la Suisse possède des instituts de recherche parmi les meilleurs au monde, et de nombreuses organisations internationales ont leur siège à Genève. Cette combinaison la prédispose à jouer un rôle de premier plan sur le terrain de la gouvernance numérique. C'est essentiel à l'heure où les tensions géopolitiques augmentent dans l'espace numérique, les données étant devenues une source de pouvoir majeure. On constate également l'émergence d'une compétition technologique planétaire, notamment sur le terrain de l'intelligence artificielle. Aussi le Conseil fédéral a-t-il fait de la numérisation une priorité thématique de sa stratégie de politique extérieure et défini dans la stratégie extérieure numérique suisse[69] les quatre champs d'action suivants: gouvernance numérique, prospérité et développement durable, cybersécurité et autodétermination numérique.

En matière de gouvernance numérique, la Suisse s'engage pour une régulation modérée et souhaite faire de la Genève internationale le premier pôle mondial de la numérisation et des technologies d'avenir. Les acteurs non étatiques occupent une place de choix dans ce contexte et participeront activement à la recherche de solutions. Sur le plan de la prospérité et du développement durable, il s'agit d'instaurer au niveau international des conditions-cadres propices à l'économie numérique et aux nouvelles technologies. Dans le cyberespace, la Suisse s'engage pour le respect du droit international et encourage le dialogue avec le secteur privé sur les règles de conduite à observer dans le cyberespace. Enfin, l'autodétermination numérique vise principalement à promouvoir une gestion responsable des données ainsi qu'à renforcer l'autodétermination numérique des individus.

---

68 Renforcement des efforts cantonaux contre la cybercriminalité et la pédocriminalité (ccdjp.ch)

69 Stratégie de politique extérieure numérique (eda.admin.ch)

5.4 Premières sanctions de l'UE contre les auteurs de cyberattaques

L'UE a fait usage en 2020, pour la première fois, de la boîte à outils cyberdiplomatique (*Cyber-Diplomacy-Toolbox*)[70] adoptée en 2019 et imposé des sanctions à l'égard des responsables présumés de cyberattaques.

Deux personnes et une entité liée au service de renseignement militaire russe (GRU) ont ainsi fait l'objet d'une interdiction de pénétrer sur le territoire de l'UE et d'un gel des avoirs. Cette sanction faisait suite à leur participation à la cyberattaque lancée en 2015 contre le Parlement fédéral allemand, au cours de laquelle une importante quantité de données avaient été volées. Il a par ailleurs été interdit à des tiers de mettre des fonds à disposition des personnes et de l'entité sanctionnées[71].

Des sanctions similaires avaient été prononcées peu avant contre six personnes et trois entités de nationalité chinoise, russe ou nord-coréenne, pour avoir participé aux campagnes Wannacry, NotPetya et CloudHopper ainsi qu'aux cyberattaques déployées contre l'Organisation pour l'interdiction des armes chimiques (OIAC) et contre le réseau électrique ukrainien[72].

70 DÉCISION 2019/797 DU CONSEIL concernant des mesures restrictives contre les cyberattaques (europa.eu)

71 Malicious cyber-attacks: EU sanctions two individuals and one body over 2015 Bundestag hack (europa.eu)

72 L'UE impose les toutes premières sanctions à la suite de cyberattaques (europa.eu)